UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,892	08/10/2006	Naoto Kuroda	9319Y-1322/NP	7169

27572 7590 07/16/2008
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
WRIGHT, BRYAN F	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
07/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/549,892	**Applicant(s)** KURODA, NAOTO
	Examiner BRYAN WRIGHT	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 10 August 2006.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-19 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-19 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 16 September 2005 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 1/3/2008, 9/16/2005.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAIL ACTION

1. This action is in response to the original filing of August 10, 2006. Claims (1-19) are pending and have been considered below.

Priority

2. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) - (d) is acknowledged.

The application is filed on August 10, 2006 but is a 371 case of PCT/JPO4/03520 application filed 3/17/2004 and has a foreign priority application filed on 03/17/2003.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 18 and 19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

a. Claim 18 and 19 recites "**a program for making a computer**", as such claim 18 and claim 19 is directed to "**a program**" for which is non-statutory subject matter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-14 and 16-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Arnold et al. (US Patent No. 5,440,723 and Arnold hereinafter).

5. As to claim 1, Arnold teaches a **method of preventing virus infection by detecting the virus infection in a network, comprising steps of:**

providing a decoy accessible through the network to a computer that monitors intrusion of a virus (i.e., … teaches deploying a decoy to capture virus [item C, fig. 2]);

receiving access to said decoy through the network, to obtain communication information and to detect intrusion of the virus (i.e., … teaches deploying a decoy to capture virus [item C, fig. 2]);

detecting a virus source computer based on the communication information obtained with respect to the virus intrusion when the virus intrudes into the decoy (i.e., … identify portions of the virus [item D, fig. 2]);

and making an antivirus attack on the virus source computer through the network for suppressing operation of the virus (i.e., … teaches a “cleanup” function such that active virus activity is revoked [col. 21, lines 20-40]).

6. As to claim 2, Arnold teaches a **method of preventing virus infection where: said decoy is one or more of a decoy folder stored in a storage unit, a decoy application stored in the storage unit, and a server formed virtually in the storage unit** (i.e., ... teaches a decoy program installed on a computer system [col. 2, lines 5-12]).

7. As to claim 3, Arnold teaches a **method of preventing virus infection where said attack is made by imposing a high load on the virus source computer** (i.e., … teaches anomaly detection [col. 4, lines 60-67] Those skilled in the art would recognize virus are anomalies in current system activities. Anomaly detection as such is pattern recognition such that a particular anomaly will coincide with a particular pattern. Particular patterns are indicative of the presence of a virus).

8. As to claim 4, Arnold teaches a **method of preventing virus where said high load is imposed on the virus source computer by increasing traffic of said computer** (i.e., … teaches anomaly detection [col. 4, lines 60-67]Those skilled in the art would recognize virus are anomalies in current system activities. Anomaly detection as such is pattern recognition such that a particular anomaly

will coincide with a particular pattern. Particular patterns are indicative of the presence of a virus).

9. As to claim 5, Arnold teaches a **method of preventing virus infection said high load is imposed on the virus source computer by sending a large number of requests to which a CPU of said computer should respond** (i.e., … teaches anomaly detection [col. 4, lines 60-67]Those skilled in the art would recognize virus are anomalies in current system activities. Anomaly detection as such is pattern recognition such that a particular anomaly will coincide with a particular pattern. Particular patterns are indicative of the presence of a virus).

10. As to claim 6, Arnold teaches a **system for preventing virus infection by detecting the virus infection in a network, comprising:**

a decoy means that can be accessed through the network (i.e., … teaches deploying a decoy to capture virus [item C, fig. 2]);

a communication information analysis means that detects intrusion of a virus into said decoy means, and then on detecting virus intrusion, detects a virus source computer based on communication information obtained when the virus intrudes (i.e., … teaches deploying a decoy to capture virus [item C, fig. 2]);

and a computer attack means that makes an antivirus attack on the virus source computer through the network, for suppressing operation of

the virus (i.e., … teaches a “cleanup” function such that active virus activity is revoked [col. 21, lines 20-40]).

11. As to claim 7, Arnold teaches a **system for preventing virus infection where said decoy means is one or more of a decoy folder stored in a storage unit, a decoy application stored in the storage unit, and a server formed virtually in the storage unit** (i.e., ... teaches a decoy program installed on a computer system [col. 2, lines 5-12]).

12. As to claim 8, Arnold teaches a **system for preventing virus infection where said computer attack means imposes a high load on the virus source computer** (i.e., … teaches anomaly detection [col. 4, lines 60-67]Those skilled in the art would recognize virus are anomalies in current system activities. Anomaly detection as such is pattern recognition such that a particular anomaly will coincide with a particular pattern. Particular patterns are indicative of the presence of a virus).

13. As to claim 9, Arnold teaches a **method of preventing virus infection in a system for preventing virus infection where said computer attack means imposes the high load on the virus source computer by increasing traffic of said computer** (i.e., … teaches anomaly detection [col. 4, lines 60-67] Those skilled in the art would recognize virus are anomalies in current system activities. Anomaly detection as such is pattern recognition such that a particular anomaly

will coincide with a particular pattern. Particular patterns are indicative of the presence of a virus).

14. As to claim 10, Arnold teaches a **system for preventing virus infection where said computer attack means imposes the high load on the virus source computer by sending a large number of requests to which a CPU of said computer should respond** (i.e., … teaches anomaly detection [col. 4, lines 60-67] Those skilled in the art would recognize virus are anomalies in current system activities. Anomaly detection as such is pattern recognition such that a particular anomaly will coincide with a particular pattern. Particular patterns are indicative of the presence of a virus).

15. As to claim 11, Arnold teaches a **system for preventing virus infection where:**

said system further comprises a detection report transmission means that sends a detection report to an administrator of the virus source computer (i.e., … teaches generating a report [item P, fig. 3]);

and said computer attack means continues to make the antivirus attack on the virus source computer until a countermeasure against the virus has been completed (i.e., … teaches a “cleanup” function such that active virus activity is revoked [col. 21, lines 20-40]).

16. As to claim 12, Arnold teaches a **system for preventing virus infection said decoy means is a decoy folder realized by an application provided in a decoy server that is formed virtually in a storage unit of a computer connected to the network** [col. 6, lines 60-67])

17. As to claim 13, Arnold teaches a **system for preventing virus infection where said decoy means is a decoy application realized as an application provided in a decoy server that is formed virtually in a storage unit of a computer connected to the network** (item J, fig. 3).

18. As to claim 14, Arnold teaches a **system for preventing virus infection according to one of claims 8, 9 and 10, further comprising: a message sending means that sends a message of announcing a start of the attack imposing the high load to the infected computer** (item H, fig. 3).

19. As to claim 16, Arnold teaches a **system for preventing virus infection, further comprising: a requesting means that notifies a network address of the virus source computer to another computer connected to the network and requests to said computer for making an antivirus attack on the virus source computer** (i.e., … teaches informing neighboring computers [step F, fig. 3; col. 19, lines 45-67; col. 20, lines 1-22]).

20. As to claim 17, Arnold teaches a **system for preventing virus infection by detecting the virus infection in a network, comprising: a request receiving means that receives a request for making an antivirus attack on a virus source computer** (col. 21, lines 25-40);

and a computer attack means that makes an antivirus attack on said virus source computer through the network for suppressing operation of a virus, based on said request received (i.e., … teaches a “cleanup” function such that active virus activity is revoked [col. 21, lines 20-40]).

21. As to claim 18, Arnold teaches a **program for making a computer prevent virus infection by detecting the virus infection in a network, wherein:**

said program makes said computer realize: a communication information analysis means that detects intrusion of a virus into a decoy means accessible through the network, and then on detecting virus intrusion, detects a virus source computer based on communication information obtained when the virus intrudes [fig. 2];

and a computer attack means that makes an antivirus attack on the virus source computer through the network, for suppressing operation of the virus (i.e., … teaches a “cleanup” function such that active virus activity is revoked [col. 21, lines 20-40]).

22. As to claim 19, Arnold teaches a **program for making a computer prevent virus infection by detecting the virus infection in a network, wherein: said program makes said computer perform processing of rejecting communication from a virus source computer when a network address of the virus source computer is notified** (col. 21, lines 50-60).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

23. Claim15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Arnold in view of Hill (US Patent No. 5,598,531).

24. As to claim 15, the system disclose by Arnold shows substantial features of the claimed invention (discussed in the paragraphs above), It fails to disclose:

> **A system for preventing virus infection further comprising: an alarm sound generation means that generates an alarm sound in an attacking terminal unit at a start of the attack or after the start of the attack** (claim 15).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Arnold as introduced by Hill. Hill discloses:

> **A system for preventing virus infection further comprising: an alarm sound generation means that generates an alarm sound in an attacking terminal unit at a start of the attack or after the start of the attack** (claim 15) (for purpose of virus alert Hill provides audible notification capability such that modifying Arnold's teaching of alerting neighboring system component in the event of a virus detection with Hill's audible alert capability provides means for alarm sounding in the event of a virus attack [col. 8, lines 20-26].

Therefore, given the teachings of Hill, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Arnold by employing the well known features of generating a audile sound base on the detection of a virus disclosed above by Hill, for which virus detection will be enhanced [col. 8, lines 20-26].

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is

(571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131